CLAIMS

What is claimed is:

1. A method of non-centralized zero-knowledge authentication for a computer network, comprising steps of:

establishing a first computer having a first authentication agent and a first prover agent on the computer network;

detecting a first authentication request over the computer network from a second computer having a second prover agent;

authenticating the second prover agent through a zero-knowledge identification protocol; and

promoting the second computer with a second authentication agent to perform authentication for the computer network.

2. The method of claim 1, further comprising periodically and distributing a new secret to the first and second authentication agents.

3. The method of claim 1, further comprising:

detecting a second authentication request over the computer network from a third computer having a third prover agent;

authenticating the third prover agent through a zero-knowledge identification protocol with the second authentication agent; and

promoting the third computer with a third authentication agent to perform authentication for the computer network.

4. The method of claim 1, further comprising periodically publishing encrypted numbers for the zero-knowledge identification protocol, including the steps of:

generating a first and second large prime numbers;

calculating a product of the first and second large prime numbers;

generating a secret to have a value relatively prime to the product, greater than zero and less than the product;

encrypting the product;

encrypting the secret; and

publishing encrypted values of the secret and product.

5. A method of protecting a host from unauthorized client access over a network, comprising the steps of:

creating a prover agent application on the client;

creating a verifier agent application on the host;

creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers;

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

decrypting the secret, by the prover and verifier;

decrypting the product, by the prover and verifier; and

performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access when the prover fails to demonstrate knowledge of the secret and product and granted access when the client succeeds in demonstrating knowledge of the secret and product.

6. The method of claim 5, wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations.

7. The method of claim 5, further comprising:

creating a first agent to be authenticated, the first agent having values for s, n and t, s being the secret, n being the product, and t being a size of an answer set;

creating a second agent to authenticate the first agent, the second agent having values for s, n, and t;

generating r as a random number generated by the first agent;

calculating x by the first agent, r being raised to power of t modulus n;

sending x from the first agent to the second agent;

calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1;

sending b from the second agent to the first agent;

calculating y by the first agent, y being a product of r * s raised to power of b;

sending y from the first agent to the second agent; and

determining authentication of the first agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, first equation is y^t mod n and second equation is (xv^b) mod n.

8. A system of non-centralized zero-knowledge authentication for a computer network, comprising:

two or more computers establishing the computer network, each of the computers containing an authentication agent, secret and prover agent; and

a requesting computer having a prover agent, for requesting access to the computer network, wherein the prover agent of the requesting computer and one of the authentication agents of the two or more computers engaging in a zero-knowledge authentication protocol, and wherein the requesting computer operates with an authentication agent on the computer network when the requesting computer is authenticated through the zero-knowledge authentication protocol.

9. The system of claim 8, further comprising a trusted source for periodically generating a new secret for the authentication agents of computers on the network.

10. The system of claim 8, the requesting computer comprising a cell phone.

11. The system of claim 8, the computer network comprising one or more of the Internet, LAN, communications link, and a wireless network.

12. The system of claim 8, the authentication agents and prover agents being installed on each of the computers through common software.

13. A software product comprising instructions, stored on computer-readable media, wherein the instructions, when executed by a computer, perform steps for non-centralized zero-knowledge authentication for a computer network, comprising:

instructions for establishing a first computer having a first authentication agent and a first prover agent on the computer network;

instructions for detecting a first authentication request over the computer network from a second computer having a second prover agent;

instructions for authenticating the second prover agent through a zero-knowledge identification protocol; and

instructions for promoting the second computer with a second authentication agent to perform authentication for the computer network.